Office of the Inspector General
United States Office of Personnel Management

Statement of the Honorable
Patrick E. McFarland
Inspector General

before the

Committee on Homeland Security and Governmental Affairs

United States Senate

on

"Under Attack: Federal Cybersecurity and the OPM Data Breach"

June 25, 2015

Chairman Johnson, Ranking Member Carper, and Members of the Committee:

Good morning. My name is Patrick E. McFarland. I am the Inspector General of the U.S. Office of Personnel Management (OPM). Thank you for inviting me to testify at today's hearing on information technology (IT) security at OPM. Today I will briefly describe our IT audit work, and then discuss a Flash Audit Alert recently issued by the Office of the Inspector General (OIG)

Legacy Systems and the Recent Security Breaches

In the past week, there have been assertions that OPM's legacy information systems are supported by very old technology (specifically COBOL, a mainframe programming language), and therefore could not be protected by modern security controls. However, we know from our audit work that some of the OPM systems involved in the data breaches run on modern operating and database management systems. Consequently, modern security technology such as encryption or data loss prevention could have been implemented on these specific systems.

Also, OPM has stated that because the agency's IT environment is based on legacy technology, it is necessary to complete a full overhaul of the existing technical infrastructure in order to address the immediate security concerns. While we agree in principle that this is an ideal future goal for the agency's IT environment, there are steps that OPM can take (or has already taken) to secure its current IT environment.

For example, OPM has significantly upgraded security controls to protect the perimeter of its network and prevent the type of attacks that occurred in 2014. In addition, some of OPM's most sensitive systems are compatible with additional security controls such as data encryption and other data loss prevention techniques, which could be utilized to protect OPM's systems. Moreover, implementing full two-factor authentication to access OPM's major IT systems will add an additional layer of defense that will go a long way toward preventing additional data breaches.

OIG's FISMA Work

In accordance with the Federal Information Security Management Act, commonly known as "FISMA," our office conducts an annual audit of OPM's IT security programs and practices. Although OPM has made progress in certain areas, some of the current problems and weaknesses were identified as far back as Fiscal Year (FY) 2007. We believe this long history of systemic failures to properly manage its IT infrastructure may have ultimately led to the breaches we are discussing today.

Today I will talk about three of the most significant concerns highlighted in our FY 2014 FISMA report. However, it is important to note that our report contained a total of 29 recommendations covering a wide variety of IT security topics. Only 3 of these 29 recommendations have been closed to date, and 9 of the open recommendations are long-standing issues that were rolled-forward from prior year FISMA audits.

1. Information Security Governance

Information security governance is the management structure and processes that form the foundation of a successful information technology security program. This is an area where OPM has seen significant improvement. However, some of the past weaknesses still haunt the agency today.

OPM's Office of the Chief Information Officer (OCIO) was responsible for the agency's overall technical infrastructure and provided boundary-level security controls for the systems residing on this infrastructure. However, each OPM program office historically had primary responsibility for managing security controls specific to its own IT systems. There was often confusion and disagreement as to which controls were the responsibility of the OCIO, and which were the responsibility of the program offices.

As a result of this decentralized governance structure, many security controls went unimplemented and/or remained untested, and OPM routinely failed a variety of FISMA metrics year after year. Therefore, we identified this security governance issue as a material weakness in all of our FISMA audits from FY 2007 through FY 2013.

However, in FY 2014, we changed the classification of this issue to a significant deficiency, which is less serious than a material weakness. This change was prompted by important improvements that were the result of changes instituted in recent years by OPM. Specifically, OPM has implemented a team of Information System Security Officers (ISSO) that report to the OCIO and who have responsibility for managing security for the agency's various information systems.

This new governance structure has resulted in improvement in the consistency and quality of security practices for the various IT systems owned by the agency.

Although we are optimistic that these improvements will continue, it is apparent that the OCIO continues to be negatively impacted by years of decentralized security governance, as the technical infrastructure remains fragmented and therefore inherently difficult to protect.

2. Security Assessment and Authorization

A Security Assessment and Authorization (Authorization) is a comprehensive process under which the IT security controls of an information system are thoroughly assessed against applicable security standards. After the assessment is complete, a formal Authorization memorandum is signed indicating that the system is cleared to operate in the agency's technical environment.

The Office of Management and Budget (OMB) mandates that all major Federal information systems have a valid Authorization (that is, that they have all been subjected to this *process*) every three years, unless a mature continuous monitoring system is in place (which OPM does not yet have). Although, as mentioned, IT security responsibility is being centralized under the OCIO, it is still the responsibility of OPM program offices to facilitate and pay for the Authorization process for the IT systems that they own.

OPM has a long history of issues related to system Authorizations. Our FY 2010 FISMA audit report contained a material weakness related to incomplete, inconsistent, and poor quality Authorization packages. This issue improved over the next two years, and was removed as an audit concern in FY 2012.

However, problems with OPM's system Authorizations have recently resurfaced. In FY 2014, 21 OPM systems were due for Authorization, but 11 of those were not completed on time and were therefore operating and continue to operate without a valid Authorization.[1] This is a drastic increase from prior years, and represents a systemic issue of inadequate planning by OPM program offices to assess and authorize the information systems that they own.

Although the majority of our FISMA audit work is performed towards the end of the fiscal year, it already appears that there will be a greater number of systems this year operating without a valid Authorization. In April, the CIO issued a memorandum that granted an extension of the previous Authorizations for all systems whose Authorization had already expired, and for those scheduled to expire through September 2016. Should this moratorium on Authorizations continue, the agency will have up to 23 systems that have not been subject to a thorough security controls assessment. The justification for this action was that OPM is in the process of modernizing its IT infrastructure and once this modernization is complete, all systems would have to receive new Authorizations anyway.

While we support the OCIO's effort to modernize its systems, this action to extend Authorizations is contrary to OMB guidance, which specifically states that an "extended" or "interim" Authorization is not valid. Consequently, these systems are still operating without a current Authorization, as they have not been subject to the complete security assessment process that the Authorization memorandum is intended to represent.

It is true that OMB now allows agencies to make ongoing Authorization decisions for IT systems based on the continuous monitoring of security controls – rather than enforcing a static, three-year re-Authorization process. However, OPM has not yet developed a mature continuous monitoring program. Until such a program is in place, we continue to expect OPM to re-authorize all of its IT systems every three years.

One effective way to reduce non-compliance with FISMA requirements would be for OPM to impose administrative sanctions on the program offices. We recommended that the performance standards of all OPM major system owners include a requirement related to FISMA compliance for the systems they own. Since OMB requires a valid Authorization for all Federal IT systems, we also recommended that the OPM Director consider shutting down systems that were in violation. None of the systems in violation were shut down.

Not only was a large volume (11 out of 47 systems) of OPM's IT systems operating without a valid Authorization, but several of these systems are among the most critical and sensitive applications owned by the agency.

Two of the OCIO systems without an Authorization are general support systems that host a variety of other major applications. Over 65 percent of all systems operated by OPM (not including contractor-operated systems) reside on one of these two support systems, and are therefore subject to any security risks that exist on the support systems.

[1] The OIG is the co-owner of one of these IT systems, the Audit Reports and Receivables Tracking System. This system has been reclassified as a minor system on the OPM general support system (GSS), and cannot be Authorized until the OCIO Authorizes the GSS.

Furthermore, two additional systems without Authorizations are owned by OPM's Federal Investigative Services, which is responsible for facilitating background investigations for suitability and security clearance determinations. Any weaknesses in the IT systems supporting this program office could potentially have national security implications.

As I explained, maintaining active Authorizations for all IT systems is a critical element of a Federal information security program, and failure to thoroughly assess and address a system's security weaknesses increases the risk of a security breach. We believe that the volume and sensitivity of OPM systems that are operating without an active Authorization represents a material weakness in the internal control structure of the agency's IT security program.

3. Technical Security Controls

As previously stated, our FY 2014 FISMA report contained a total of 29 audit recommendations related to a wide variety of technical controls.

There are many steps that OPM could take today to help improve the security posture of its existing technical environment. OPM has already implemented a variety of new controls and tools over the past year designed to strengthen the agency's technical infrastructure. However, in order to be effective, these tools must be installed and configured correctly, and must cover the entire technical environment. Our audit work has determined that this is not always the case.

Some of the specific technical weaknesses that we have identified include:

- Vulnerability scans – vulnerability scanning tools were not running correctly because they did not have the correct credentials, and the scans were not targeting the full environment. In addition, OPM did not have a process to track the status of vulnerabilities identified in the scans;

- System inventory – OPM has not developed a comprehensive list of minor applications that reside on the agency's general support systems. In addition, our vulnerability scan test work detected servers and databases that could not be accounted for on any system inventory;

- Personal identity verification (PIV) authentication – none of the agency's major applications require two-factor authentication via PIV credentials;

- Baseline configurations – OPM has not documented pre-approved secure configurations for the operating systems it utilizes;
- Configuration change control - OPM cannot ensure that all changes made to information systems have been properly documented and approved;

- Patch management – our vulnerability scan test work determined that numerous servers were not patched on a timely basis;

- VPN connections – VPN connections do not time out after 30 minutes of inactivity; and,

- Continuous monitoring – OPM does not have a mature continuous monitoring program and still relies on the periodic assessment of security controls.

OPM's Infrastructure Overhaul Project

In April 2014, in response to the March 2014 breach, OPM initiated a major IT overhaul. The initial plan was to make major security improvements to the existing environment and continue to operate OPM systems in their current location. During the process of implementing security upgrades, OPM determined that it would be more effective to completely overhaul the agency's IT infrastructure and architecture and move it into an entirely new environment (referred to as the Shell).

There are four phases in the Project:

- Tactical – shoring up the existing security environment
- Shell – creating the new data centers and IT architecture
- Migration – migrating all OPM systems to the new environment
- Clean-up – decommissioning existing hardware and systems

Our understanding is that the Tactical phase was completed in April 2015 and the Shell phase is underway and is expected to be completed this fall.

It is important to understand that the Tactical phase of this Project was in fact urgent, and it was absolutely critical to complete it as quickly as possible. However, the other phases of the Project are really a capital investment. These modernization efforts are indeed needed, but like any long-term investment, the Project must be carefully planned and implemented.

We support OPM's efforts to modernize and better secure its IT environment; however, we have two significant concerns with this Project, resulting in the issuance of a Flash Audit Alert.

Flash Audit Alert

The typical audit process can take up to 10 to 12 months from the start of the audit to the issuance of the final report. As part of our normal audit process, we provide a draft audit report to OPM for comment. It is a fact finding step to ensure that our audit field work is complete and accurate. We consider those comments, make any necessary changes, and incorporate them into our final audit report.

However, sometimes in the course of our work, we discover significant evidence of a critical problem that needs *immediate* attention by OPM. In those situations, we issue what is called a "Flash Audit Alert." We do not normally provide a draft of this alert to the agency for comment given the time sensitive nature of the matter.

After our auditors finished conducting their initial review of the Project, we determined (1) the situation was serious enough to issue a Flash Audit Alert and (2) because of the significance of the Project, we would provide the agency with a brief window to provide comments on the draft alert.

We provided a draft copy of our Flash Audit Alert to the Office of the Chief Information Officer (OCIO) on June 2, 2015, after verbally briefing the CIO several days before. We requested comments by June 5th, and later extended that to June 10th. By June 17th we still had not received comments, or indication that comments would be forthcoming. Because of the urgency of the situation, I issued the Flash Audit Alert without the benefit of agency comments.

The two primary concerns discussed in the Flash Audit Alert relate to (1) project management and (2) the use of a sole-source contract.

1. Project Management Activities

The most significant shortcoming of OPM's management of the Project is that it has not prepared a "Major IT Business Case" proposal (formerly known as the OMB Exhibit 300), as required by OMB for IT projects of this size and scope. Preparing an OMB proposal would require OPM to fully evaluate the costs, benefits, and risks associated with its planned Project, and present its business case to OMB to seek approval and funding.

OMB Circular A-11 Appendix 6 defines capital budgeting requirements for capital asset projects. The basic concepts are that capital asset projects require proper planning, cost/benefit analysis, financing, and risk management. This includes demonstrating that the return on investment exceeds the cost of funds used, and that the full cost of the project is appropriated before work begins. Finally, the Circular requires risk management and earned value management throughout the life-cycle of the Project to ensure that it continues to meet cost and schedule targets.

For OPM to complete this process it must first fully determine the true scope and cost of the project. However, we learned from our audit work that OPM is still evaluating its existing IT architecture, including the identification of all mainframe applications that will need to be migrated to the Shell environment. Further, other systems will need to be redesigned before they can be migrated. There are approximately 50 major IT systems in OPM's inventory, and a large number of related sub-systems. Until this evaluation is complete, OPM is not able to estimate how long it will take or how much it will cost to complete the Migration phase of the Project.

Despite this, OPM officials informed us that the Migration phase will be complete in 18 to 24 months. We believe that OPM is highly unlikely to meet this target. Many critical OPM applications (including those that process annuity payments for Federal retirees, reimburse health insurance companies for claims payments, and manage background investigations) run on OPM's mainframe computers. These applications are based on legacy technology, and will need to be completely renovated to be compatible with OPM's proposed new IT architecture.

This will be a highly complex and monumental task. OPM has a history of troubled system development projects. Despite multiple attempts OPM has failed to modernize its retirement claims processing system. Although the 2009 revamp of OPM's financial system (now called CBIS) was ultimately partially successful, it was also fraught with difficulty. The CBIS project was the main focus of agency leadership at that time. It was relatively well managed, and was subject to oversight from several independent entities, including my office, but it still required two years and over $30 million to complete.

OPM's current initiative will be far more complex than anything OPM has attempted in the past, since each individual application migration should be treated as its own project similar to these examples. Furthermore, there are many other systems besides OPM's mainframe applications that will also need to be modified to some extent to be compatible with the Shell environment.

Even more troubling is the fact that OPM has not followed basic best practices for program management including developing a project charter, a comprehensive list of stakeholders, a feasibility study and impact assessment, test plans, and other standard project management artifacts.

In addition to defining cost and schedule targets, the OMB Major IT Business Case process is intended to secure funding for major IT investments before work begins. However, OPM has already committed substantial funds toward this project without completing the process. In FY 2015 OPM has obligated approximately $32 million toward shoring up its existing IT security controls and establishing the Shell environment. In its FY 2016 budget request, OPM requested an additional $21 million from OMB for the Project.

OPM program officials told us that some of the Project's funding will come from the $21 million budget request, $5 million from the U.S. Department of Homeland Security, and from assessments on the program offices. In addition, program offices will be required to fund the migration of applications they own from their existing budgets. However, program office budgets are intended to fund OPM's core operations, not subsidize a major IT infrastructure project.

It is unlikely that OPM will be able to fund the substantial migration costs related to this Project without a significantly adverse impact on its mission unless it seeks dedicated funding through Congressional appropriation. Also, OPM's current budget approach seems to violate IT spending transparency principles promoted by OMB's budget guidance and its IT Dashboard initiative, which is intended to "shine [a] light onto the performance and spending of IT investments across the Federal Government."

Without a dedicated funding stream, there is a very high risk that funding will be inadequate to support the entire Migration phase, which is likely to be complex, time consuming, and extremely expensive. In addition, without the disciplined project management processes that are associated with the OMB Major IT Business Case process, there is a high risk that this Project will fail to meet all of its stated objectives. In this scenario, the agency would be forced to indefinitely support multiple data centers, further stretching already inadequate resources, possibly making both environments less secure, and increasing costs to taxpayers. This outcome would be contrary to the stated goals of creating a more secure IT environment at a lower cost.

The best chance for a successful modernization of OPM's IT environment is to develop and execute a comprehensive plan based on accepted project management disciplined processes.

OPM's Response to the Flash Audit Alert

OPM submitted a response to our Flash Audit Alert on June 22, 2015. First, OPM disagreed that they should follow industry best practices. OPM has its own Systems Development Life Cycle (SDLC) and the agency believes it is adhering to that policy. However, the OIG would like to point out that OPM is not complying with its own SDLC, which requires similar documentation as industry best practices.

Second, OPM implied that the agency did not need to submit a Major IT Business Case to OMB because (1) it would take too long and the Tactical phase had to be implemented quickly and (2) the agency worked closely with OMB, and thus already had OMB's approval. OPM noted that "submitting an initial Major IT Business Case document requires anywhere from eight months to a year of research, consultations, discussion, and effort." OPM repeatedly stated that it would have delayed their work to prepare this document.

Although this is indeed a time consuming process, the OIG firmly believes that work on this Project should not move forward without this kind of careful planning. Indeed, we are alarmed that the agency sees such vital planning steps (like defining the scope and costs of the entire Project) as administrative impediments to action.

Finally, OPM stated that another reason supporting not having a Major IT Business Case is that the migration of the systems are part of existing IT Investments (that is, IT projects for which a Major IT Business Case has been prepared) that are already being tracked on OMB's IT Dashboard by the program offices that own those systems.

The OIG disagrees. The OMB concept is that there should be transparency and accountability on IT projects. First, not every OPM IT system is associated with an IT Investment that is tracked on the OMB IT Dashboard. Essentially, OPM is not treating this modernization as a single project, but rather multiple projects conducted by the individual program offices. This approach prevents transparency and accountability at the agency level by having the program offices subsume the costs. This also reverses the progress OPM has made towards centralizing its IT functions within the OCIO. Under this model, no one person is accountable for the success of the Project.

2. Sole-Source Contract

OPM has secured a sole-source contract with a vendor to manage the infrastructure improvement project from start to finish. Although OPM completed a Justification for Other Than Full and Open Competition (JOFOC) to justify this contract, we do not agree that it is appropriate to use this contract for the entire Project.

The initial phase of the Project covered the procurement, installation, and configuration of a variety of software tools designed to improve the IT security posture of the agency (the Tactical phase). We agree that recent security breaches at OPM warranted a thorough and immediate reaction to secure the existing environment, and that the JOFOC was appropriate for this activity. However, we do not agree that it is appropriate to use a sole-source contract for the long-term system development and migration efforts.

OPM officials informed us that the reason for using the sole-source contract for the long-term was to ensure continuity. The OCIO believes the same vendor that helped build the infrastructure should be responsible for migrating applications into that environment.

Federal Acquisition Regulation § 6.302 outlines seven scenarios where contracting without full and open competition may be appropriate, two of which relate to an unusual and compelling urgency and national security implications. There is no exception to the requirement for full and open competition for vendor continuity for the convenience of the agency.

The current vendor may well be chosen as the successful bidder through full and open competition when the Migration and Clean-up phases begin. Without subjecting the remainder of this process to competition, there is a high risk that project costs will be inflated. Further, it is highly unlikely that any single vendor is qualified for the Migration phase. OPM's information systems are supported by a wide variety of operating systems, databases, and programming languages. Each individual application migration will likely require dedicated contractor support by a vendor that specializes in the specific technology supporting that system.

The Migration and Clean-up phases are not responses to a crisis situation, as the Tactical phase was. Therefore, we believe that OPM should subject the remainder of the project to contracting vehicles other than the sole-source contract used for the Tactical and Shell phases.

OPM's Response

In its June 22nd response to the Flash Audit Alert, OPM implies that the OIG misunderstands the scope of the contract. However, our auditors reviewed both the JOFOC and the contracts, and it is clear in the documents that OPM intends to use the sole-source contract for the full scope of the Project. Further, the CIO personally informed the OIG staff that the contract was for all four phases of the contract because continuity was important to the success of the Project. In fact, if OPM intended to have multiple contractors work on the Project, then requests for proposals (known as RFPs) for that work would already have been published, considering that the Migration phase is supposed to be completed by 2017.

Conclusion

While I fully support OPM's efforts to modernize its IT environment, I am concerned that there is a high risk that its efforts will ultimately be unsuccessful. For example, if the Migration phase fails, the results could be catastrophic. The agency could end up with half of its systems in the new Shell environment and half of its systems in the legacy environment. Neither of the environments would be fully secure, and OPM would be in a position where it is forced to pay indefinitely for the overhead costs of both infrastructures.

System development projects by their very nature are complex and prone to failure. Even with the application of strict project management techniques, many projects either fail entirely, or are only partially successful. Even so, there is a chance that this effort will ultimately succeed given time, leadership, and strong project management.

I am happy to answer any questions you may have.